



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON THE SUBGROUPS OF AN ABELIAN GROUP

BY G. A. MILLER

THE main object of this paper is to develop a convenient formula by means of which all the possible subgroups of a given abelian group may be directly written down. For this purpose it appears desirable to present some well known facts relating to the independent generators in a form which is especially suited to our point of view. The list of these facts is more complete than would be necessary for what follows, since it is hoped that the somewhat new form of many of them will make the list of interest and value in itself.

1. Fundamental Theorems. Any abelian group (G) is the direct product of a number of cyclic subgroups $C_1, C_2, \dots, C_m$. The groups $C_1, C_2, \dots, C_m$ may always be so chosen that the order of each of them is a power of a single prime number. In this case the number of these subgroups and their orders are fully determined by G provided none of them is the identity.* That is, if G is also the direct product of the cyclic groups $C'_1, C'_2, \dots, C'_{m'}$, where the order of each of these groups is again a power of a single prime, then it follows that $m' = m$ and that the groups $C_1, C_2, \dots, C_m$ and $C'_1, C'_2, \dots, C'_{m'}$ can be so arranged that the order of C_α is equal to that of C'_α ($\alpha = 1, 2, \dots, m$). In particular when the order of G is a power of a prime the orders of $C_1, C_2, \dots, C_m$ are completely determined by G , for each must be a power of a single prime. In any case, the orders of $C_1, C_2, \dots, C_m$ are *invariants* of G whenever each of them is a power of a prime.

When the order of each of the independent generating cyclic subgroups $C_1, C_2, \dots, C_m$ is a power of a single prime we obtain the largest possible number of independent subgroups of G . That is, *neither G nor any of its subgroups can have more than m independent generators*. We proceed to find the smallest number of independent generators of G . The given subgroups $C_1, C_2, \dots, C_m$ may be arranged in rows such that the orders of all of those in one row are powers of the same prime and that the order of each is equal to or greater than the order of the one which follows it in the same row. In case the

* Unless the contrary is stated it will be assumed that the order of every subgroup exceeds unity. Otherwise, the number of independent generating subgroups is indeterminate, as the identity can be added any number of times to these subgroups.

rows do not contain the same number, the vacant places may be filled by the identity. Arranging these rows in the form of a rectangle we have

$$\begin{array}{ccccccc} C_1, & C_2, & \cdot & \cdot & \cdot & C_a \\ C_{a+1}, & C_{a+2}, & \cdot & \cdot & \cdot & C_{2a} \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \end{array}$$

By forming the products of all those in each column we obtain *a independent* cyclic subgroups such that the order of each is divisible by the orders of all those which follow it. These subgroups form the smallest possible number of generating cyclic subgroups of G . The orders of these subgroups are commonly called *the invariants* of G , since any other system of independent generating cyclic subgroups in which every order is divisible by every following order is composed of *a* groups of the same orders respectively. It may be observed that *a* is the largest number of invariants in a Sylow subgroup* of G while *m* is equal to the sum of the numbers of invariants of all the Sylow subgroups of G . It is clear that the independent generators of G may be so selected that their number has any arbitrary value from *a* to *m*, but this number can have no other value. Moreover, G cannot be generated by less than *a* cyclic subgroups even if these subgroups are not independent.

Whenever the independent generators of G are so chosen that each of them is divisible by all those which follow it their number must be *a*, and when the order of each is a power of a single prime their number must be *m*. These two numbers are equal only when the order of G is a power of a single prime. Since the former method leads to the smallest number of invariants it seems appropriate to call the orders of these independent generators *the invariants* of G , although the latter method has some advantages. The choice of invariants such that their number lies between *a* and *m* seems less natural. We evidently arrive at the *a* invariants if we choose the independent generators in the ordinary way; *i.e.* start with an operator of highest order and then select any other operator such that the two generate the largest possible subgroup. The orders of two independent generators of this subgroup are the first two invariants of G . If we add to this subgroup another operator so that the three generate the largest possible subgroup, we arrive at the third invariant, etc.

* If the order of a group is divisible by p^a (p being a prime), but not by p^{a+1} , its subgroups of order p^a are called Sylow subgroups.

A marked difference between the two given methods of arriving at the invariants of G should perhaps be emphasized; viz., the orders of the independent generators of G are completely determined by m , but not by a . That is, if two sets of m independent generating cyclic subgroups of G were given the orders of the subgroups of one set would be the same as those of the other; but if two sets of a independent generating cyclic subgroups of G were given the orders of those of one set could generally vary a great deal from the orders of those of the other. The necessary and sufficient condition that the orders of these two sets be the same is that each of the Sylow subgroups of G contain the same number of invariants.

If G is the direct product of a series of subgroups $G_1, G_2, \dots, G_\lambda$ we may select a set of independent generators of G by taking any set of independent generators of each one of these subgroups. Suppose that $G_1, G_2, \dots, G_\lambda$ are the Sylow subgroups of G . Any operator (t) of G will have a constituent, which may be the identity, from each one of these subgroups and the order of t will be the product of the orders of these constituents. In order to determine the number of the operators of a given order in G it is only necessary to determine the number of operators of a given order in each of the Sylow subgroups. That is, if the order of t is $p_1^{a_1} p_2^{a_2} \dots p_\lambda^{a_\lambda} (p_1, p_2, \dots, p_\lambda \text{ being prime numbers})$, the number of operators of G whose order is equal to the order of t is the product of the numbers of operators of orders $p_1^{a_1}, p_2^{a_2}, \dots, p_\lambda^{a_\lambda}$ in the respective Sylow subgroups of G . We proceed to determine this number.

2. Number of operators of a given order in a group of order p^m .

Let G be any group of order p^m whose invariants are $p^{a_1}, p^{a_2}, \dots, p^{a_\gamma}$ ($a_1 \geq a_2 \geq \dots \geq a_\gamma > 0$). Let $m_1 = \gamma$ represent the number of invariants $\leq p$, m_2 the number of those $\leq p^2, \dots, m_{a_1}$ the number of those $= p^{a_1}$. To determine the number of the operators of order p^β ($1 \leq \beta \leq a_1$) it is only necessary to find the order of the group generated by all the operators whose orders divide p^β and subtract from this number the order of the group formed by all the operators whose orders divide $p^{\beta-1}$. That is, the number of operators of order p^β in G is equal to *

$$p^{m_1 + m_2 + \dots + m_\beta} - p^{m_1 + m_2 + \dots + m_{\beta-1}} = p^{m_1 + m_2 + \dots + m_{\beta-1}} (p^{m_\beta} - 1).$$

* Heffter, *Crelle*, vol. 119 (1898), p. 261; Netto, *Vorlesungen über Algebra*, vol. 2 (1900) p. 248.

This result may also be obtained by observing that all the operators whose orders divide p^β constitute a group which has m invariants; m_β of these are equal to p^β while the remaining $m - m_\beta$ are the invariants of G which are less than p^β . If $\alpha_\rho \equiv \beta > \alpha_{\rho+1}$ the order of this group is p^M , where $M = \beta m_\rho + \alpha_{\rho+1} + \dots + \alpha_\gamma$. The order of the group which is composed of all the operators whose orders divide $p^{\beta-1}$ is found in the same way and the difference of these orders is the number of operators of order p^β which are contained in G .

3. Number of different types of subgroups in a group of order p^m . Let G have the same invariants as in the preceding paragraphs. It is well known that any ρ powers of p , such as $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_\rho}$, are the invariants of some subgroup of G , provided $\beta_1 \equiv \alpha_1, \beta_2 \equiv \alpha_2, \dots, \beta_\rho \equiv \alpha_\rho^*$. As these conditions are necessary as well as sufficient, $\rho \equiv \gamma$. Hence the number of different types of subgroups having just ρ invariants ($\rho > 1$) is given by the formula

$$\begin{array}{ccc} \lambda_\rho = 0 & & \lambda_3 = \lambda_4 \quad \lambda_2 = \lambda_3 \\ \sum & \dots & \sum \quad \sum \alpha_1 - \lambda_2 \\ \lambda_\rho = \alpha_\rho - 1 & & \lambda_3 = \alpha_3 - 1 \quad \lambda_2 = \alpha_2 - 1 \end{array}$$

There are evidently just $\alpha_1 + 1$ cyclic subgroups†. For instance, the group whose invariants are p^9, p^3, p^2, p^2 contains 9 cyclic subgroups, 24 which have two invariants, 39 which have three invariants, and 54 which have four invariants. From the fact that $\lambda_\rho = 0$ whenever $\alpha_\rho = 1$, it follows that *the number of the different types of subgroups which have ρ invariants is equal to the number which have $\rho - 1$ invariants whenever $\alpha_\rho = 1$.*

The number of the different types of subgroups which have just ρ invariants may be directly obtained, without the use of a formula, as follows: First suppose that all the invariants after the first are equal to p . There are clearly α_1 such subgroups. Then suppose that the second invariant is p^2 while all those which follow it are equal to p . As we may suppose that the invariants are always arranged in order of magnitude, there are $\alpha_1 - 1$ such subgroups. Continuing to multiply the second invariant by p until it is equal to p^{α_2} , we find the number of different types of subgroups in which all the invariants after the first two are equal to unity. This number is clearly equal to $\alpha_1 + (\alpha_1 - 1) + \dots + (\alpha_1 - \alpha_2 + 1)$. We then increase the third invariant successively by a multiple of p , while the first and second invariant can have all possible values such that the first $\equiv$ the second $\equiv$ the third. Continuing this process

* Burnside, *Theory of groups of finite order*, 1897, p. 58.

† The identity is here included among the cyclic subgroups of G .

until we arrive at p invariants we obtain all the possible types of subgroups which have just p invariants.

When the order of G is not a power of a prime number the number of its different types of subgroups is the product of the number of the different types of subgroups in its Sylow subgroups. The identity and the entire group are included under the term subgroup in this statement. Hence the given formula can be directly employed to determine the number of different types of subgroups in any abelian group.

4. Total number of subgroups in a group of order p^m . It will only be necessary to determine the number of the subgroups whose invariants are $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_p}$ ($\beta_1 \equiv a_1, \beta_2 \equiv a_2, \dots, \beta_p \equiv a_p$).^{*} Let $s_1, s_2, \dots, s_p$ represent the independent generators of such a subgroup, the orders of these independent generators being $p^{\beta_1}, p^{\beta_2}, \dots, p^{\beta_p}$ respectively. For s_1 we may choose any one of the $(p^{m_{\beta_1}} - 1)p^{m_1 + m_2 + \dots + m_{\beta_1} - 1}$ operators of G whose order is p^{β_1} . We proceed to determine the number of ways in which s_2 can be chosen. It is clear that we may take any operator of order p^{β_2} except those which generate the same subgroup of order p that s_1 does. As the number of the latter is equal to $p - 1$ times the order of the group composed of all the operators in G whose orders divide $p^{\beta_2 - 1}$, the number of ways in which s_2 may be chosen is

$$(p^{m_{\beta_2}} - 1)p^{m_1 + m_2 + \dots + m_{\beta_2} - 1} - (p - 1)p^{m_1 + m_2 + \dots + m_{\beta_2} - 1},$$

or
$$(p^{m_{\beta_2}} - p)p^{m_1 + m_2 + \dots + m_{\beta_2} - 1}.$$

Similarly, we may take any operator of order p^{β_3} for s_3 with the exception of those which generate a group of order p contained in $\{s_1, s_2\}$. The number of the latter is equal to $p^2 - 1$ times the order of the group composed of all the operators of G whose orders divide $p^{\beta_3 - 1}$. Hence the third independent generator can be chosen in

$$(p^{m_{\beta_3}} - p^2)p^{m_1 + m_2 + \dots + m_{\beta_3} - 1}$$

ways. The number of ways in which s_p can be chosen is

$$(p^{m_{\beta_p}} - p^{p-1})p^{m_1 + m_2 + \dots + m_{\beta_p} - 1}.$$

The product of all these numbers gives the number of ways in which the

* The independent generators and the invariants are always supposed to be arranged in order of magnitude, the largest coming first.

independent generators of such a subgroup may be chosen from the operators of G . If we divide this product by the number of ways in which these independent generators can be chosen within the subgroup we obtain a quotient which represents the number of the subgroups of G which are of type $(\beta_1, \beta_2, \dots, \beta_p)$.

If we put $A = \sum_{x=0}^{x=\rho-1} (\rho - x)(m_{\beta_{\rho-x+1}} + m_{1+\beta_{\rho-x+1}} + \dots + m_{-1+\beta_{\rho-x}})$, this quotient is

$$\frac{(p^{m_{\beta_1}} - 1)(p^{m_{\beta_2}} - p) \dots (p^{m_{\beta_p}} - p^{\rho-1}) p^A}{\text{Same expression except that } m \text{ is replaced by } n},$$

where n_a represents the number of the invariants which are $\equiv p^a$ in the required subgroups, $m_{\beta_{\rho+1}} = m_0 = n_{\beta_{\rho+1}} = n_0 = 0$, and $m_{\beta_{\rho-x+1}} + \dots + m_{-1+\beta_{\rho-x}} = 0 = (n_{\beta_{\rho-x+1}} + \dots + n_{-1+\beta_{\rho-x}})$ whenever $\beta_{\rho-x+1} = \beta_{\rho-x}$.

By means of this formula we can determine the total number of subgroups of a given type in G . A preceding formula gives the number of possible types. Hence the two formulas together enable us to determine all the possible subgroups of a group of order p^m . When the order of G is not a power of a prime number the number of its subgroups is the product of the numbers of the subgroups in the Sylow subgroups of G . Hence the given formulas may be employed to determine the number of subgroups in any abelian group.

STANFORD UNIVERSITY,
FEBRUARY 1904.